Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1645 11/05/14

~ WiFi Name Grounds Plane ~ People Are Talking! ~ New Apple Malware!
~ WAM!, Twitter Join Up! ~ Workbench Replacements! ~ Call of Duty Reviews
~ Final AmigaOS Edition! ~ "Dark" Network Targeted ~ WireLurker Stopped!

~ Mozilla FX10 Browser! ~ "Dark Web" Is Challenge ~ Blizzard Shows Shooter

-* Security Breach Not Detected *-
-* Exhumed Atari Games End Up on eBay! *-
-* Extremist Use, Social Networks "In Denial" *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

Mercifully, the elections are over here in the States - at least this latest round. We're no longer being barraged with campaign attacks ads and political mailings. However, I don't think President Obama and his Democratic cronies are too happy that they don't have more time to attempt to sway voters. Final outcome: the American people have spoken, and showed their displeasure with Obama and his party. Hopefully, this will result in a lot of positive change!

Until next time...

=~=~=~=

AmigaOS 4.1 Final Edition Available Before the End of 2014

Hyperion Entertainment is pleased to announce the imminent availability of "AmigaOS 4.1 Final Edition" for all supported platforms.

AmigaOS 4.1 was released in September of 2008 and has seen no less than 6 free major updates and at least 88 smaller updates released through AmiUpdate.

New functionality in AmigaOS 4.1 Final Update includes but is not limited to:
Extended memory functionality (beneficial for all supported platforms even those platforms which cannot be equipped with more than 2GB)

Most powerful console for AmigaOS
New Intuition features
New Workbench features
Much improved DOS

New unified graphics library with RTG support which allows for (current and future) very substantial general and platform specific performance optimizations e.g. through the use of on-chip DMA engines (present on recently released hardware going back to the Sam440)

Updated Python port

Installation graphics, new icons and back-drops by Martin Merz
Countless minor updates, new other functionality and bug-fixes.

AmigaOS 4.1 Final Edition requires NO previous version of AmigaOS 4.x and is a stand-alone product, quite possibly the most affordable version of AmigaOS ever to be released.

This now allows current users of AmigaOS 4.1 to install a complete original version of AmigaOS 4.1 without subsequently needing to download or apply 6 updates and countless minor updates.

Users are nevertheless recommended to register their copy of AmigaOS 4.1 Final Edition on the Hyperion Entertainment website as this will be required for downloading possible future updates and bug fixes.

An updated SDK for developers which exposes all new OS functionality to developers, is being worked on.

Hyperion Entertainment wishes to thank all those developers and contributors who have furthered AmigaOS development over the years and especially those that have worked tirelessly on delivering "AmigaOS 4.1 Final Edition" to customers before the end of 2014.

Our thanks go out to all of our supporters and loyal customers who can rest assured that work on AmigaOS 4.2 is ongoing apace albeit somewhat behind schedule due to the fact that substantial time had to be allocated for supporting new upcoming exciting hardware platforms. We appreciate your support!

AmigaOS Final Edition has gone gold and is in production at this time.

Suggested retail price is 29,95 EUR (SRP includes German VAT, may vary depending on your location).

New Replacement Workbench 3.1 Disk Sets

Our customers have regularly been asking for replacement Workbench floppy disk sets since their older disks have either become corrupted or worn out due to age. About a year ago, we approached our friends at Cloanto to enquire about a possible solution. As a result, we are pleased to announce the immediate availability of new Workbench 3.1 Floppy Disk Set

This new distribution comes with some minor enhancements and updates:

- Updated C/Version (Y2K patch)
- Addition of Libs/workbench.library (for A-4000T 3.1 ROMs and 3.X ROMs)
- Updated S/Startup-Sequence (for 3.X ROMs)
- Updated Installer 44.10 and FastFileSystem 45.9 (to support larger disks)
- Installer itself is now part of the system installation (inside the Utilities directory)

As you may notice these disk sets are also compatible with the Amiga 4000T (workbench.library on floppy) so there is no requirement any longer to have two distributions of Workbench 3.1 media.

Thank you to Cloanto for their support in this project

=~=~=~=

->In This Week’s Gaming Section - The Legend of Zelda Majora’s Mask!
"""""""""""""""""""""""""""""""" Call of Duty: Advanced Warfare Reviews!
Exhumed Atari Carts Land on Ebay!
And much more!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Nintendo Plans Remake Encore with ’Majora’s Mask 3D’

Nintendo has enjoyed great success with its reissue of "The Legend of Zelda: Ocarina of Time" in 2011, still the 3DS’s highest-rated title to this day (Metacritic), and oft-credited with a significant contribution to a successful rejuvenation of the then-ailing handheld console.

Next in the series in terms of chronological release - the fictional timeline starts getting a little convoluted after "Ocarina of Time" - is 2000’s N64 title "The Legend of Zelda: Majora’s Mask."

It continues the childhood adventures of franchise hero Link but tackles deeper themes and is presented using more sophisticated graphics.

In a special online broadcast made on November 5, Nintendo president Satoru Iwata confirmed that the celebrated title would make a much-requested transition to 3DS for early 2015.

That helps make the first half of the year even more significant for current and prospective 3DS and 2DS owners, with "Monster Hunter 4 Ultimate" due during the same period.

While "Majora’s Mask" could be used to drive adoption of the New Nintendo 3DS, a more powerful version of what will then be a four-year-old handheld, another cult remake - "Xenoblade Chronicles New 3DS" - is already in position to do just that in 2015, exclusive as it will be to the upgraded machine.

In fact, what with it targeting the more established regular 3DS platform, there is a good chance that "Majora’s Mask 3D" will end up reaching a wider audience than its ancestor.

That’s because the first version required a special memory expansion pack on N64, going on to achieve an estimated 3.3 million lifetime sales; remake predecessor "Ocarina of Time 3DS" enjoyed a rapturous reception and was able to surpass the 3.3m mark within two years of availability.

Call of Duty: Advanced Warfare Review Roundup

The high-tech future of Call of Duty has arrived, and it’s looking pretty bright. Marking a return to form after last year’s disappointing Call of Duty: Ghosts, Sledgehammer Games’ Call of Duty: Advanced Warfare (available now for Xbox One, Xbox 360, PS4, PS3 and PC) is earning big praise for its kinetic player mobility, explosive campaign and addictive multiplayer modes. Our full review is on the way, but in the meantime, here’s what some of gaming’s top critics are saying about the highly-anticipated shooter.

Polygon’s Arthur Gies awarded Advanced Warfare a 9 out of 10, claiming that the shooter takes just enough design risks to move the franchise forward. He notes that while the story is a bit predictable, the new mechanics made possible by the player’s Exo suit switch things up significantly.

"Speaking strictly from level and encounter design and mission variety, Advanced Warfare is the best campaign the series has seen since Infinity Ward re-imagined the franchise with Modern Warfare in 2007"

"There’s less safety, less predictability, and it combines with some of the best map design the series has seen."

"Much has been made of House of Cards actor Kevin Spacey’s turn as Jonathan Irons, the CEO of a paramilitary-oriented corporation named Atlas, but his performance tends toward over-the-top."

Jeff Gerstmann of Giant Bomb gave Advanced Warfare 4 stars out of 5, commending the title’s refreshed gameplay, detailed graphics and engaging campaign. Gerstmann was particularly impressed with the game’s heightened sense of movement, claiming that it "makes every other game in the franchise feel obsolete by comparison."

"It probably doesn’t sound like much, but being able to get around the map more quickly and change your elevation with ease actually makes a huge difference."

"The game benefits a lot from Spacey’s performance, which looks extremely realistic in cutscenes and only slightly less realistic in-game."?

"The campaign is another six-hour romp through a war-torn world. It’s straightforward as ever, which is a little disappointing considering the series did better with player choice and branching in the campaign back in Black Ops II."

While IGN is waiting to spend more time in multiplayer before delivering a final verdict on Advanced Warfare, reviewer Brian Albert’s review-in-progress of the game is largely positive. Like his peers, Albert speaks highly of the game’s Exo suit mechanics, weapon variety and creative multiplayer.

"The Exo suit is the kind of change I was looking for in Call of Duty multiplayer. It s intuitive, fun, and it affects everything you do."
"Pores, hair, and creases in skin are all rendered in great detail, to the point where I knew, just by seeing how a character s face displayed

shock and horror, that bad news was coming."

"The biggest hindrance to Advanced Warfare s story is the way it fails to establish its characters human relationships."
"The one design decision seemingly made in the name of variety that I felt harmed my enjoyment of Advanced Warfare is that we don t get access to the full range of Exo movement abilities in every campaign level."

Gamespot’s Miguel Concepcion gave Advanced Warfare an 8 out of 10, speaking highly of the game’s rich mulitplayer, impressive introduction sequence and high-tech gear. Like other reviewers, though, Concepcion felt that the title’s inconsistent storytelling holds the campaign back a bit.

"Sledgehammer Games crafted an opening that does everything a great first chapter is meant to do: it welcomes you with big-budget bravado, offers control tips without excessive hand-holding, and establishes the tone of the campaign."

"Sledgehammer should also be commended for designing original multiplayer maps without borrowing heavily from the single-player locales. "?

"I was left hoping that this Call of Duty had a point to its uncharacteristically cartoon-like dramatics, but it instead leaves you with an unsatisfying conclusion driven by a tonally inconsistent script."

"The campaign is an entertaining ride as a whole, but being able to progress through most of it with a classic Call of Duty approach is wholly unfortunate, as it contradicts the expectations set by the futuristic motifs of the initial chapter."

In his 4-star review, Ludwig Kietzmann gave Advanced Warfare big props for embracing Call of Duty’s over-the-top nature to the fullest in the name of fun. One of his few gripes was in the campaign, as Kietzmann wished for more opportunities to use the game’s many cool gadgets in every mission.

"Whether it’s in the rich and varied multiplayer mode, or the frantic, thrill-a-minute single-player campaign, you’re constantly relying on cool weapons and combat data to make taking lives easier."

"The futuristic EXO suit that encases your soldier in strong metal limbs and a boosting backpack lets you juke, bounce and dash aggressively through the air like a rocket-powered bayonet. It feels truly three-dimensional and liberating and punchier than Titanfall, if you care to compare."

"It’s a shame these [new] mechanisms come across as guest stars, because their use feels so fitting with Advanced Warfare’s unabashed science fiction shooting gallery."

Blizzard Reveals Shooter ’Overwatch’ at BlizzCon

After tackling online strategy and role-playing games, the company behind "World of Warcraft" is taking aim at the shooter genre.

Blizzard Entertainment Inc. announced plans Friday to release a multiplayer shoot-’em-up PC game called "Overwatch." The reveal kicked off BlizzCon, the company’s fan-centric celebration where more than 25,000 attendees are competing in game matches, dressing in costumes and bagging swag at the Anaheim Convention Center.

Blizzard’s chief of story and franchise development, Chris Metzen, said "Overwatch" marks the first new franchise in 17 years from the creator of such long-running game series as the fantasy role-playing saga "World of Warcraft," gothic slasher "Diablo" and sci-fi strategy game "StarCraft."

"You guys know that with Blizzard games, we like to find genres and game types that we’re in love with and take the best elements of those and really amplify it," game director Jeff Kaplan told the BlizzCon crowd. "You saw us do that with a strategy genre, a massively multiplayer online game, and most recently a collectable card game."

"Overwatch" will feature original superhero-like characters with various skills such as mechanized gorilla Winston, winged healer Mercy and robotic monk Bastion blasting each other in six-versus-six matches on a futuristic, cartoony rendition of Earth.

"The story takes place something like 60 years in the future," Metzen said. "It’s far enough in the future that we have flying cars, ray guns and all the technology you’d want to have, but it’s not far enough that it feels too exotic."

A beta test for "Overwatch" will launch in 2015 and a demonstration of the game is available at the convention this weekend, Metzen said.

"Overwatch" will join Blizzard’s growing game portfolio, which includes such newcomers as the "Warcraft"-themed collectable card game "Hearthstone" and the battle arena game "Heroes of the Storm" featuring characters from other Blizzard games.

Blizzard also announced plans Friday for the first "Hearthstone" expansion and a version coming to the Android devices.

The developers declined to specify whether the business model of "Overwatch" would be subscription-based like "World of Warcraft," free-to-play like "Hearthstone" or stand-alone like "Diablo."

StarCraft II’s Final Episode Unveiled, Legacy of the Void Welcomed to BlizzCon

StarCraft II’s final episode has been officially unveiled today on the main BlizzCon stage. StarCraft II: Legacy of the Void will put players into the shoes, err, claws of Heirarch Artanis as he works to unite the Protoss factions and retake Aiur. The expansion will also feature several features in addition to the new campaign and units: Automated Tournaments, two-player cooperative Archon Mode, and the cooperative hero-based mode Allied Commanders. Best of all? Legacy of the Void is a standalone product.

Covering the individual changes to Zerg, Protoss and Terran might be a bit beyond the scope of this announcement article, but count on each faction gaining new units, as well as major changes to make certain

things more or less viable.

The campaign, though... the campaign is interesting. With the final chapter of StarCraft II we finally escape the drama of Kerrigan and Raynor, or at least I hope that’s the case. Suddenly there’s a new enemy in the universe and hopefully that means the story actually feels meaningful. Up until now it has seemed like Blizzard’s been unaware that their story may be a hugely contributing factor towards StarCraft II’s failure to recapture the excitement of the original Perhaps a legitimate, epic Protoss storyline will save the day.

I’d also love to hear more about Automated Tournaments, Archon Mode and Allied Commanders, but there aren’t many details about the game out just yet. Automated Tournaments is rather self-explanatory, offering a daily tournament for players to participate in - so long as they have a few hours to invest. Archon Mode makes sense too - two players controlling one base against two enemy AI. It’s useful for coaching and general fun. What is Allied Commanders though? A Warcraft III style mode?

Unfortunately, StarCraft II: Legacy of the Void does not have a release window yet. Blizzard may perhaps be unwilling to dedicate to a 2015 release date even if that’s the plan, considering they’re still trying to build up the audience of Heart of the Swarm. Players can, however, register for the beta starting today. The beta is absolutely confirmed for 2015. Do that by registering through your Battle.net account.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Exhumed Atari Cartridges from New Mexico Dig Site Land on Ebay

One man’s garbage is another man’s treasure, and so it goes with roughly 100 Atari 2600 cartridges dug up from a landfill in Alamogordo, New Mexico that are now available on Ebay. Following decades old reports that trucks would use the cover of night to dump unsold games, system hardware, and peripherals into a dump site, Microsoft recently financed a documentary in which the disposed items were unearthed.

After jumping through hoops and regulatory hurdles to tear into a landfill that had been covered with concrete over 30 years ago, the dig finally took place as filmmakers recorded the event. Of main interest were E.T the Extra-Terrestrial cartridges. It’s considered by many to be the worst game of all time, largely the result of a hurried development, though it was never known for sure if earlier reports of their burial were actually true.

It turned out they were, and in addition to E.T. games, the dig also uncovered several other games and gear. About 100 of the games are up on Ebay with bids starting at around $50 and ballooning to over $500 for the suddenly coveted E.T. title.

The Internet Archive Now Lets You Play 900+ Classic Arcade Games In Your Browser

Looking for a nice little burst of nostalgia on this fine Saturday evening? Don t feel like going through the process of installing MAME and lurking for ROMs, but still want to get your classic arcade on?

Back in December of last year, the Internet Archive (in their effort to backup the entire digital world, one bit at a time) launched a Console Living Room that offers up browser-friendly emulators for a pretty shocking number of consoles from the 70s/80s. Want to play some Atari 2600? Here you go. Sega Genesis? Yup!)

This weekend, they ve introduced a whole new category: The Internet Arcade. 900+ classic arcade games, no quarters required.

It s all a part of the JSMESS project, an effort to emulate as many systems as possible in Javascript, of all languages. As they put it, they want to make computer history and experiences as embeddable as movies, documents, and audio .

Do they all work seemlessly? Nah you ll almost certainly spot a bug or two. Many are missing sound. But it ll get better in time and for now, just the fact that they got MAME working in a browser, sans any hefty plugins/runtime environments, is damned impressive.

(Pro tip: it can be a bit weird to figure out a game s controls in MAME some times. The 5 key lets you insert a coin; the 1 key is usually the Player 1 start button. Arrows are usually used for directional stuff, with CTRL/ALT/SPACE used for the three primary buttons. Beyond that, you ll have to mash buttons a bit to figure it out [or hit TAB to dive into the key configurations])

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Security Contractor Breach Not Detected for Months

A cyberattack similar to previous hacker intrusions from China penetrated computer networks for months at USIS, the government's leading security clearance contractor, before the company noticed, officials and others familiar with an FBI investigation and related official inquiries told The Associated Press.

The breach, first revealed by the company and government agencies in August, compromised the private records of at least 25,000 employees at the Homeland Security Department and cost the company hundreds of millions of dollars in lost government contracts.

In addition to trying to identify the perpetrators and evaluate the scale of the stolen material, the government inquiries have prompted concerns about why computer detection alarms inside the company failed to quickly notice the hackers and whether federal agencies that hired the company should have monitored its practices more closely.

Former employees of the firm, U.S. Investigations Services LLC, also have raised questions about why the company and the government failed to ensure that outdated background reports containing personal data weren't regularly purged from the company's computers.

Details about the investigation and related inquiries were described by federal officials and others familiar with the case. The officials spoke only on condition of anonymity because they were not authorized to comment publicly on the continuing criminal investigation, the others because of concerns about possible litigation.

A computer forensics analysis by consultants hired by the company's lawyers defended USIS' handling of the breach, noting it was the firm that reported the incident.

The analysis said government agencies regularly reviewed and approved the firm's early warning system. In the analysis, submitted to federal officials in September and obtained by the AP, the consultants criticized the government's decision in August to indefinitely halt the firm's background investigations.

USIS reported the cyberattack to federal authorities on June 5, more than two months before acknowledging it publicly. The attack had hallmarks similar to past intrusions by Chinese hackers, according to people familiar with the investigation. Last March, hackers traced to China were reported to have penetrated computers at the Office of Personnel Management, the federal agency that oversees most background investigations of government workers and has contracted extensively with USIS.

In a brief interview, Joseph Demarest, assistant director of the FBI's cyber division, described the hack against USIS as "sophisticated" but said "we're still working through that as well." He added: "There is some attribution" as to who was responsible, but he declined to comment further.

For many people, the impact of the USIS break-in is dwarfed by recent intrusions that exposed credit and private records of millions of customers at JPMorgan Chase & Co., Target Corp. and Home Depot Inc. But it's significant because the government relies heavily on contractors to vet U.S. workers in sensitive jobs. The possibility that national security background investigations are vulnerable to cyber-espionage could undermine the integrity of the verification system used to review more than 5 million government workers and contract employees.

"The information gathered in the security clearance process is a treasure chest for cyber hackers. If the contractors and the agencies that hire them can't safeguard their material, the whole system becomes unreliable," said Alan Paller, head of SANS, a cybersecurity training school, and former co-chair of DHS' task force on cyber skills.

Last month, the leaders of the Senate Homeland Security and Governmental Affairs Committee, Tom Carper, D-Del., and Tom Coburn, R-Okla., pressed

OPM and DHS about their oversight of contractors and USIS' performance before and during the cyberattack.

Another committee member, Sen. Jon Tester, D-Mont., said he worried about the security of background check data, telling AP that contractors and federal agencies need to "maintain a modern, adaptable and secure IT infrastructure system that stays ahead of those who would attack our national interests."

The Office of Personnel Management and the Department of Homeland Security indefinitely halted all USIS work on background investigations in August. OPM, which paid the company $320 million for investigative and support services in 2013, later decided not to renew its background check contracts with the firm. The move prompted USIS to lay off its entire force of 2,500 investigators. A company spokesperson complained that the agency has not explained its decision. Representatives from OPM and DHS declined comment.

Last month, the federal Government Accounting Office ruled that Homeland Security should re-evaluate a $200 million support contract award to USIS. The GAO advised the department to consider shifting the contract to FCi Federal, a rival firm, prompting protests from USIS.

In the private analysis prepared for USIS by Stroz Friedberg, a digital risk management firm, managing director Bret A. Padres said the company's computers had government-approved "perimeter protection, antivirus, user authentication and intrusion-detection technologies." But Padres said his firm did not evaluate the strength of USIS' cybersecurity measures before the intrusion.

Federal officials familiar with the government inquiries said those assessments raised concerns that USIS' computer system and its managers were not primed to rapidly detect the breach quickly once hackers got inside.

The computer system was probably penetrated months before the government was notified in June, officials said. Cybersecurity experts say attacks on corporate targets often occur up to 18 months before they are discovered and are usually detected by the government or outside security specialists.

Still, USIS noted its own security preparations "enabled us to self-detect this unlawful attack."

Padres said the hackers attacked a vulnerable computer server in "a connected but separate network, managed by a third party not affiliated with USIS." He did not identify the outside company.

Former USIS workers told the AP that company investigators sometimes stored old or duplicate background reports that should have been purged from their laptops. The reports contained sensitive financial and personal data that could be used for blackmail or to harm government workers' credit ratings, the former workers said.

Former USIS employees who worked with the federal personnel office said the system they used directed users to purge old reports. But the workers said USIS and OPM rarely followed up with spot checks. Employees who worked on systems with the Homeland Security Department said these had no similar automatic warning function and spot checks were rare. The company insisted spot checks were regularly performed.

Several former USIS workers said they were told nothing by the company about the cyberattack for two months after the breach was exposed. In emails obtained by AP, company workers were ordered to change their passwords without explanation.

The USIS spokesperson said the government directed the company's decision to keep silent about the breach. Experts said companies often withhold such information for both security and management reasons.

"Employees may not like it," Paller said, "but from a business perspective, that's what companies do."

'Trojan Horse' Bug Lurking in Vital US Computers Since 2011

A destructive Trojan Horse malware program has penetrated the software that runs much of the nation s critical infrastructure and is poised to cause an economic catastrophe, according to the Department of Homeland Security.

National Security sources told ABC News there is evidence that the malware was inserted by hackers believed to be sponsored by the Russian government, and is a very serious threat.

The hacked software is used to control complex industrial operations like oil and gas pipelines, power transmission grids, water distribution and filtration systems, wind turbines and even some nuclear plants. Shutting down or damaging any of these vital public utilities could severely impact hundreds of thousands of Americans.

DHS said in a bulletin that the hacking campaign has been ongoing since 2011, but no attempt has been made to activate the malware to damage, modify, or otherwise disrupt the industrial control process. So while U.S. officials recently became aware the penetration, they don t know where or when it may be unleashed.

DHS sources told ABC News they think this is no random attack and they fear that the Russians have torn a page from the old, Cold War playbook, and have placed the malware in key U.S. systems as a threat, and/or as a deterrent to a U.S. cyber-attack on Russian systems   mutually assured destruction.

The hack became known to insiders last week when a DHS alert bulletin was issued by the agency s Industrial Control Systems Cyber Emergency Response Team to its industry members. The bulletin said the BlackEnergy penetration recently had been detected by several companies.

DHS said BlackEnergy is the same malware that was used by a Russian cyber-espionage group dubbed Sandworm to target NATO and some energy and telecommunications companies in Europe earlier this year. Analysis of the technical findings in the two reports shows linkages in the shared command and control infrastructure between the campaigns, suggesting both are part of a broader campaign by the same threat actor, the DHS bulletin said.

The hacked software is very advanced. It allows designated workers to

control various industrial processes through the computer, an iPad or a smart phone, sources said. The software allows information sharing and collaborative control.

Social Networks ’In Denial’ on Extremist Use: GCHQ Chief

Social media sites have become "the command-and-control networks of choice for terrorists", a senior British spy said Tuesday, warning that some US technology companies are "in denial" over the issue.

Robert Hannigan, the new head of electronic spying agency GCHQ, used a Financial Times article to urge Silicon Valley big names to give security services more help in the fight against Islamic State (IS) jihadists.

The rare public comments by a senior intelligence officer will fuel the debate ignited by US leaker Edward Snowden over how much access governments should have to personal online information and what steps social networks should take to regulate content.

Classified information released by former intelligence analyst Snowden in 2013 revealed that GCHQ played a key role in covert US surveillance operations worldwide, including monitoring huge volumes of online and phone activity worldwide.

While Hannigan did not name firms directly, he highlighted militants’ use of Twitter, Facebook and WhatsApp and referred to graphic online videos showing the final moments of Western hostages executed by the IS group.

"However much they dislike it, they have become the command-and-control networks of choice for terrorists and criminals," he wrote in the FT.

"To those of us who have to tackle the depressing end of human behaviour on the Internet, it can seem that some technology companies are in denial about its misuse."

The comments were backed by Downing Street as "important".

"The prime minister very much shares the view that’s being expressed there around the use of web-enabled Internet access technologies by violent and extremist groups amongst others and the need to do more," David Cameron’s official spokesman told reporters.

Government officials have held a series of meetings on the issue with firms such as Google and Facebook, most recently last month.

Campaigners said the security services already have ample access to online information.

Eric King, deputy director of Privacy International, called Hannigan’s comments "disappointing".

"Before he condemns the efforts of companies to protect the privacy of their users, perhaps he should reflect on why there has been so much criticism of GCHQ in the aftermath of the Snowden revelations," he said.

"GCHQ s dirty games - forcing companies to hand over their customers

data under secret orders, then secretly tapping the private fibre optic cables between the same companies' data centres anyway - have lost GCHQ the trust of the public, and of the companies who services we use."

Eva Galperin of the Electronic Frontier Foundation, a non-profit organisation which campaigns for online civil liberties, also criticised the remarks.

"Their powers are already immense. I think that asking for more is really quite disingenuous," she told BBC radio.

In 2013, Cameron's government scrapped planned legislation dubbed a "snoopers' charter" which would have compelled mobile phone and Internet service providers to retain extra data amid opposition from coalition partners the Liberal Democrats.

But Home Secretary Theresa May has vowed to revive it if the prime minister's Conservatives win next May's general election outright.

Hannigan's comments came less than a week after he started work with GCHQ's reputation in the spotlight after Snowden's revelations.

In a farewell speech last month, his predecessor, Iain Lobban, launched a robust defence of GCHQ staff, saying their mission was "the protection of liberty, not the erosion of it".

Britain is on a high state of alert due to the fear of attacks linked to the IS group in Syria and Iraq, where it is taking part in international air strikes.

In August, Britain's threat level from international terrorism was raised to severe, the second highest level, meaning that an attack is thought to be highly likely.

Police said last month they were taking down around 1,000 pieces of illegal content from the Internet every week including videos of beheadings and torture.

WAM! And Twitter Tackle Problem Of Online Harassment Of Women

WAM!, Women, Action & The Media, is working with Twitter to combat online harassment of women.

Zelda Williams received tweets from Twitter trolls telling her they were glad her father, actor Robin Williams, committed suicide. Chrissy Teigen, after a tweet about American gun violence, received death threats on the social media site. And Jezebel writer Lindy West, after appearing on a talk show to explain rape culture, received verbal abuse and - you guessed it - rape threats on Twitter.

You don t have to be female to get harassed on social media, but women disproportionately receive the most severe forms of online abuse, according to a recent Pew report. Although Twitter, bowing to increased outside pressure, created a "Report Abuse" button last summer, the feature is an imperfect solution to a growing problem.

The Cambridge, Massachusetts-based group WAM! (Women, Action & the

Media), in collaboration with Twitter Inc., hopes to do something about that. On Thursday the group announced a pilot project to collect data on gendered harassment that will allow it to work with Twitter - both on understanding the harassment and how to improve Twitter s responses to it. It will also look into how that gendered harassment intersects with harassment of people of color, women in the LGBT community and "fat women," in the group's words.

In a form they're providing called the "WAM Twitter Harassment Reporting Tool," the organizers ask women who have been the target of harassment on Twitter to answer questions, such as what form the harassment took, whether they fear for their personal safety, and how many times they've reported the harassment to Twitter.

Using this information, WAM! promises to act as an advocate to speed up Twitter's response to the complaints, as well as to use the data to help Twitter improve its responses:

"We're using this pilot project to learn about what kind of gendered harassment is happening on Twitter, how that harassment intersects with other kinds of harassment (racist, transphobic, etc.), and which kinds of cases Twitter is prepared (and less prepared) to respond to. We'll then work with Twitter to improve their responses to the harassment of women on their platform."

Jaclyn Friedman, the executive director of WAM! and author of "Yes Means Yes!: Visions of Female Sexual Power and a World Without Rape," talked with International Business Times about the pilot program.

How did your collaboration with Twitter happen? Who are you working with specifically?

We're in conversation with some folks at Twitter as part of the newly formed Speech and Safety Coalition, a group of organizations and advocates working to make social media safer for all kinds of women. This project grew out of those conversations.

You announced the pilot program on Thursday. When does it end?

We're not sure. We think it will run for a month, give or take. It depends on how long it takes to get enough data to be meaningful when we analyze it.

Could you say more about how gendered harassment functions with other harassment ? Why is that important?

We know that when women of color are targeted, they are targeted in ways that are specifically racist, and they also experience the harassment in different ways because of their previous experiences with racism. Similar can be said of trans women, fat women, queer women, etc. We're interested in the kinds of context that influence how harassment functions to silence women, and those mechanisms work differently for different groups of women.

Besides Twitter s implementation of a report abuse button, has it done anything else to address gendered harassment on Twitter? How would you describe what it has in place now?

I don't want to speak for Twitter, but I know they're working on a number of things right now to address gendered harassment. It's a work in

progress, and we’re happy to be working with them.

What would you like women’s experiences and oppressed subjects’ experiences to look like online in the future?

This is a free speech issue. Our hope is to make our new "public squares," which are all privately held companies, places where all women can speak freely without being silenced by fear and abuse.

Dark Network of Illegal Websites Targeted by U.S. and European Police

An international task force executed a series of raids and arrests in 16 countries on Friday aimed at shutting down a secret network of websites. These so-called dark sites matched anonymous sellers and buyers in a thriving black market for illicit goods and services including drugs, stolen credit cards, weapons and killers for hire.

The investigation, nicknamed Operation Onymous, targeted mostly sellers and deactivated upward of 50 websites like Silk Road 2.0, Mr. Quid s Forum, Paypal Center, Cannabis Road Markets and Blue Sky, according to Europol.

Across Europe and the United States, at least 17 sellers were arrested this week and law enforcement authorities seized Bitcoins valued at $1 million along with gold, cash and drugs, according to Troels Oerting, who heads Europol s cybercrime center.

The investigation had been underway for several months as the dark market mushroomed, Mr. Oerting said, And we had to find a way to see how we could strike back.

Investigations and coordinated by Europol in the various European countries with raids that started on Wednesday and Thursday but blossomed into a broad sweep by Friday. Working in English as a common language, investigators made arrests in Eastern and Western Europe, including France, Germany, Spain, and England.

Mr. Oerting declined to say how law enforcement authorities had cracked the dark websites despite the sites use of anonymous Tor software. But its penetration by law enforcement agencies, which have now managed to lift the anonymity coveted by users for both good and bad purposes, sent shivers through users of a formerly darkened corner of the web universe.

The Tor browser, originally developed by the United States Naval Research Laboratory, is an open source project that permits people to use the Internet without revealing their location. It is used not only for dark purposes, but also by those such as whistle-blowers and political activists seeking to avoid censorship by government agencies.

Tor cannot be entered through regular web browsers. To access Tor, users need special software known as the Tor Browser bundle. The name Tor is an acronym for the onion router, a reference to the layers of encryption on the network.

Those targeted in the sweep were part of a thriving yet secret global marketplace, which included web pages designed to mimic conventional online retail giants, even down to offering a system to review and rate

the quality of service.

The business model is to create web stores on these hidden services and then use the normal transport to deliver it, Mr. Oerting said.

If you need 10 grams of cocaine they will deliver it with a courier or a mailman. You can pay for it with Bitcoin, or a credit card, Mr. Oerting added. The problem is that in this system the criminals cheat on each other.

The authorities did not release the names of those arrested while investigators probed information seized from the computers of the sellers to target the buyers of illegal goods. In due time, Mr. Oerting said, a second wave of raids and arrests could be expected.

In a related arrest in California this week, a criminal complaint described how an undercover Homeland Security agent successfully infiltrated the support staff for Silk Road 2.0 and regularly interacted directly with its operator, who used the pseudonym Defcon.

On Wednesday, the authorities arrested Blake Benthall, 26, in San Francisco and charged him with operating Silk Road 2.0, the online marketplace created to be a successor to the original Silk Road website, a black market for drug sales and other illegal activity that used Bitcoins.

Silk Road 2.0 was formed last November to fill the void left by the government s closing of the original website, according to a criminal complaint filed in Federal District Court in Manhattan.

In recent months, Silk Road 2.0 had about 150,000 monthly active users, and generated at least $8 million in monthly sales and at least $400,000 in monthly commissions, the authorities said.

Mr. Benthall appeared before a magistrate judge in San Francisco on Thursday and agreed to be transferred to Manhattan, said Daniel Blank, his federal public defender in San Francisco. Mr. Blank added that he expected Mr. Benthall would seek bail in New York. Mr. Benthall faces charges that include conspiracies of narcotics trafficking, computer hacking and money laundering.

As recently as Oct. 29, the complaint said, Silk Road 2.0 was dominated by offerings for illegal narcotics, with more than 14,000 listings for Drugs, including 1,654 for Psychedelics and 1,921 for Ecstasy.

Recent listings, the complaint said, also included 100 grams of Afghan Heroin Brown Power for Bitcoins worth about $4,555, a fake Danish passport for Bitcoins worth about $2,414 and a fake New Jersey driver s license for Bitcoins worth about $98.

According to Mr. Oerting, there was no limit to the products and services on the illegal sites, which apparently included offers of killers for hire.

The scope is basically everything is for sale, everything that is stolen, Mr. Oerting said. You might even buy a stolen car. But in general they were selling anything you would want to send with a normal mailman, the fastest business mode, he said.

Now the website and others seized in the global investigation open to a splash page with the words, THIS HIDDEN SITE HAS BEEN SEIZED." Alongside it are the logos of various government agencies including the F.B.I. and Europol.

’Dark Web’ Drug Site Challenge Law Enforcement

No sooner had authorities announced the shuttering of an alleged illegal online drug bazaar than another popped up claiming to take its place.

Welcome to the "dark Web," an increasingly popular corner of the Internet where thousands of computer users from around the globe interact anonymously and, in many cases, illegally.

On Thursday, the U.S. Department of Justice charged a 26-year-old San Francisco man with operating Silk Road 2.0, an anonymous website that authorities say rang up $8 million in monthly drug sales.

On Friday, an underground website calling itself Silk Road 3.0 Reloaded claimed to be open for business on the TOR network, which is linked globally through special browsers that encrypt Internet traffic. Several other websites on the TOR network also claimed to be open for drug transactions.

The dark Web poses new and formidable challenges for law enforcement agencies around the world that have been dealing for decades with more conventional international drug trafficking. The reach and anonymity of these 21st century Internet operations is difficult to penetrate. Silk Road and copycats on the TOR network are not readily visible through popular Internet search sites. The buyers and sellers don’t exchange cash, dealing instead in often untraceable digital currencies, usually Bitcoin. So there are no banking records for investigators to subpoena.

"As long as the dark Web exists, there will always be people who set up places to engage in wrongdoing," said Joseph DeMarco, a defense attorney and former federal prosecutor who headed the computer crimes section of the U.S. attorney’s office in New York. DeMarco said he was skeptical that a single "global solution" would be found to stop illegal activity on the TOR network.

"There will always be an arms race between the bad guys and law enforcement," DeMarco said.

Those who created and support the TOR network say it’s a way to protect online users’ privacy in the digital age. TOR boasts that none of its websites will appear in Google search.

"TOR was created to protect people’s privacy and anonymity, and we don’t condone its use for these illegal activities," said Roger Dingledine, who co-created the TOR network originally for the U.S. Navy.

But investigators around the globe say the network is also a place of flagrant and profligate illegal activity of all sorts from prostitution to arms trafficking and they vow to crack down.

"Underground websites such as Silk Road and Silk Road 2.0 are like the Wild West of the Internet, where criminals can anonymously buy and sell

all things illegal," said Homeland Security Investigations Executive Associate Director Peter Edge.

The day after the FBI announced it had arrested Blake Benthall in San Francisco, European authorities said they arrested 16 other people in Ireland and Germany as part of the crackdown on dark Web sites.

"They believed that they could not be touched. We've proven that is not right," said Troels Oerting, head of the European police agency's cybercrimes division. "Expect to see more of these operations in the future.

Oerting expects more than 55 websites will be shut down.

In addition to the Silk Road site, authorities say they have seized or shut down other virtual marketplaces with names such as Hydra, Cloud Nine, Pandora and Blue Sky. Police in Europe seized $1 million in digital currency and $225,000 worth of cash, drugs, gold and silver.

The FBI said it seized $100,000 in cash from Benthall's San Francisco apartment and allege that he earned $400,000 in monthly commissions on $8 million in monthly sales.

Benthall, who has worked as a computer software engineer, was in federal custody in San Francisco awaiting U.S. marshal transportation to New York to face felony charges of conspiracy to traffic in controlled substances, computer hacking, conspiracy to traffic in fraudulent identifications and money laundering. Benthall has not entered a plea.

Palo Alto Networks Discovers New Malware Affecting Apple Devices

Cyber security software maker Palo Alto Networks Inc said it discovered a new family of malware affecting Apple Inc's OS X desktop and iOS mobile operating systems. The new family of malware, dubbed WireLurker, "marks a new era in malware across Apple's mobile and desktop platforms," the company said in a statement. WireLurker can install third-party applications on non-jailbroken iOS devices and can attack iOS devices through OS X via USB devices, the company added. Apple was not immediately available for comment.

WireLurker Mac OS X Malware Shut Down

WireLurker is no more.

After causing an overnight sensation, the newly disclosed family of Apple Mac OS X malware capable of also infecting iOS devices has been put to rest. Researchers at Palo Alto Networks confirmed this morning that the command and control infrastructure supporting WireLurker has been shut down and Apple has revoked a legitimate digital certificate used to sign WireLurker code and allow it to infect non-jailbroken iOS devices.

WireLurker is gone, said Ryan Olson, intelligence director at Palo Alto. What s important about this attack is the precedent it set by some new techniques presented in this attack that were actually pretty

effective.

The ultimate goal of the WireLurker attacks, which were limited to China, is unknown but the malware was capable of stealing system information and data stored on mobile devices. Other personal information such as credentials or banking transactions was spared.

Researchers at Palo Alto Networks discovered and dubbed the threat WireLurker because it spreads from infected OS X computers to iOS once the mobile device is connected to a Mac via USB. The malware analyzes the connected iOS device looking for a number of popular applications in China, namely the Meitu photo app, the Taobao online auction app, or the AliPay payment application. If any of those are found on the iOS device, WireLurker extracts its and replaces it with a Trojanized version of the same app repackaged with malware.

Patient zero is a Chinese third-party app store called Maiyadi known for hosting pirated apps for both platforms. To date, Palo Alto researchers said, 467 infected OS X apps have been found on Maiyadi and those apps have been downloaded more than 350,000 times as of Oct. 16 by more than 100,000 users.

Palo Alto says this is the biggest scale threat to OS X ever seen; the malware was in its third iteration already, and it was the first malware to infect installed iOS apps in the same way as a traditional virus would. Most worrisome is its ability to beat non-jailbroken iOS devices, doing so by installing Trojanized applications signed with a legitimate enterprise digital certificate.

The attackers did so by using a likely stolen legitimate certificate from a Chinese enterprise participating in Apple s iOS Developer Enterprise Program. The program allows iOS application developers access to iOS developer libraries and other resources and distribute homegrown signed iOS apps to users via an enterprise provisioning profile, rather than uploading it to the Apple App Store.

Apple has since revoked the certificate used by WireLurker from Hunan Langxiong Advertising Decoration Engineering Co. Ltd.

While WireLurker was relatively benign and currently under wraps, with hundreds of thousands of infected in the wild, the potential for future damage is there.

 This was widely distributed, Olson said. There are lots of infected Macs out there and someone is certainly going to find one and reverse engineer it to understand how works and possibly launch their own attacks.

Palo Alto has been researching WireLurker since June 1 when it was reported to them by a developer at Tencent, a Chinese Internet service portal, who found suspicious files and processes running on his Mac and iPhone. Palo Alto researcher Clau Xiao soon put all the pieces together after similar reports of strange applications and enterprise provisioning profiles showing up on non-jailbroken iPhones and iPads began popping up on Chinese developer and Apple forums. The link between all the users, Palo Alto learned, was Maiyadi. The security company said almost all of the 467 infected Mac OS X were uploaded to the Maiyadi app store between April 30 and June 11; all were Trojanized and repackaged with WireLurker.

Three of the top 10 downloaded Mac OS X apps on the store were downloaded 20,000 times each; the app titles include The Sims 3, International Snooker 2012, Pro Evolution Soccer 2014, Angry Birds and NBA 2K13.

Palo Alto said the attackers were not hosting the malware on Maiyadi servers, instead on cloud storage services hosted by Huawei and Baidu. Once a victim downloads an infected app on OS X and runs it, the malware drops a number of executables, libraries and configuration files before the app runs; the apps, Palo Alto said, perform as expected. Launch daemons dropped by WireLurker manage communication with a command and control server located in Hong Kong and hosted at www[.]comeinbaby[.]com. Only the third and most current version has deployed custom encryption to secure communication with command and control; the first two versions handled this in plain text, Palo Alto said.

Another launch daemon attacks iOS devices over USB, monitoring for connections between iOS and Mac OS X and then determining jailbreak status by trying to connect to AFC2 or Apple File Conduit which allows root access to the device. If it exists, the malware knows the device is jailbroken and behaves one way. If non-jailbroken, a repacked malicious iOS app is installed from backup and signed with the legitimate certificate. The iOS apps are installed to the device through the same iTunes protocol used for legitimate apps. On jailbroken devices, the Trojan will also inject malicious code into system applications and will query all contacts, phone numbers and Apple IDs on the device and send them to the command and control server.

The Trojan evolved quickly, Palo Alto said. Version A, generated on April 30, consisted of just the original malicious files used to Trojanize Mac OS X apps on Maiyadi. Version B appeared on May 7 and distributed through the WireLurker command and control infrastructure. It was the first to download and install malicious iOS apps, but only for jailbroken devices. In August, Version C appeared and it contained malicious iOS apps for jailbroken and non-jailbroken iOS devices and was the first to encrypt C&C communication.

Two processes are always running on computers and mobiles infected with WireLurker, Palo Alto said. One checks for updates with C&C, and the other is available for downloading additional IPA iOS application archive files and monitoring for connections over USB.

Palo Alto has observed only the once command and control server, which hosts code updates, iOS apps, processes reports on WireLurker status, accepts uploads of stolen data and device information from both platforms.

What we have here is likely a really talented bunch of Mac and iOS developers who probably have not developed a lot of malware in the past and didn t understand a lot about evading detection, Olson said. They were trying things out and had success. Their motivation is unclear yet, but we might find out more.

Mozilla Announces "FX10" Browser Built From Ground up For Web Developers

For web developers, page basic layout work is typically done in

development environments provided by companies Adobes Systems Inc. or Microsoft Corp. But actual testing of sites and your scripts for them is often done in browsers.

Microsoft, the Mozilla Foundation, and Google Inc. (among others) have long offered developers tools of varying complexities to analyze websites, allowing debugging and tuning. But such tools had always been cobbled onto the underlying consumer-aimed web-browsing product.

The Mozilla Foundation has offered up an interesting idea, revealing that it’s about to launch a brand new Firefox family browser built from the ground up to cater to the developer crowd. The new browser will be made available Nov. 10 and is being advertised on Twitter Inc.’s microblogging platform under the tag "#fx10".

Mozilla writes:

We’ve redesigned the browser by looking at it through a completely new filter to put developers interests first. It s built by developers for developers so you can debug the whole Web, allowing you to more easily build awesome Web experiences. It also integrates some powerful new tools like WebIDE and the Firefox Tools Adapter.

Note, both Google (maker of the Chrome web browser) and Mozilla (maker of the Firefox web browser) had previously released browsers primarily targeted at developers (e.g. the nightly Chromium and Firefox Aurora channels, respectively), but those releases were simply early versions of upcoming consumer releases, designed to keep developers in the loop about upcoming standards support and features (and to ensure compatibility).

By contrast the new browser scraps the consumer design ethos and ostensibly will look to solely focus on browser-tools/interfaces that allow for faster web development, including compatibility testing.

Al-Quida Free Terror Nettwork’ Wi-Fi Hotspot Grounds Plane

American Airlines Flight 136 from LAX to London was delayed on Sunday night after someone in the vicinity picked an inappropriate name for their Wi-Fi hotspot.

The drama began when a passenger on Flight 136 from Los Angeles International Airport to London Heathrow discovered a wireless connection named "Al-Quida Free Terror Nettwork [sic]."

The passenger alerted a flight attendant who passed the concern over to the flight crew.

Passenger Kevin Simon told Daily Mail Online that the crew informed passengers there was a ’minor security issue’ as the plane was held in position for an hour and a half before returning to the terminal gate.

While passengers were very much kept in the dark, learning what had happened later from the news, Simon did reveal how on-board security was alert to the situation, saying:

While at the baggage carousel a few passengers were talking, and a lady

who had been near the front said that she was sitting near the air marshalls, and when the event happened, both of them jumped up and got busy, with one of them stationing himself in front of the cockpit door.

Fellow passenger and Head of Digital for the UK Government, Anthony Simon, took to social media to air his frustrations over the delay:

Thanks to the idiot who did this meaning I won’t get back to London for another day.

Ultimately the flight, which was scheduled to depart at 7:50pm on Sunday, was delayed for 17 hours as investigators looked into possible threats. With none found, the flight was eventually cleared for departure at 1pm yesterday.

An American Airlines spokesman confirmed the flight was delayed "out of an abundance of caution" while local law enforcement said its investigation revealed that "no crime was committed and no further action will be taken."

And even though no physical harm was caused, the disruption to the flight, passengers and airport were very real.

We know that the average person is not too fussy about the networks they connect to, as Sophos’s James Lyne discovered on his recent Warbiking tour.

While travelling around major cities such as London and San Francisco, Lyne discovered that thousands of people would connect to networks with names such as "FreePublicWiFi", "Free Internet" and even "DO NOT CONNECT" with devices that were themselves poorly secured through the adoption of old security standards.

You can read 10 wireless security tips over on the Sophos website.

Hopefully, in this case, the owner of the ’Al-Quida’ hotspot was nothing more than a misguided joker, proving that we cannot implicitly trust the names of Wi-Fi networks (and making the point that no security-related joke is ever funny in an airport where staff and police are required to investigate every potential breach of security).

=~=~=~=

Atari Online News, Etc.